Remarks

The Office Action mailed March 30, 2006 has been carefully reviewed and the foregoing amendment has been made in consequence thereof.

Claims 16-22, 24, 25, and 27-32 are now pending in this application. Claims 16-20, 24, 25, 27-31 stand rejected. Claims 21 and 22 stand objected to. Claim 32 is newly added. No additional fee is due for newly added Claim 32.

The rejection of Claims 16-22, 24, 25, and 27-31 under 35 U.S.C. § 112, first paragraph, is respectfully traversed. Claims 16, 25, 28, and 30 have been amended to address the issues raised by the Examiner at paragraph 5 of the Office Action. For the reasons set forth above, Applicants respectfully request that the Section 112 rejections of Claims 16-22, 24, 25, and 27-31 be withdrawn.

The rejection of Claims 16, 19-22, 24, and 30 under 35 U.S.C. § 112, second paragraph, is respectfully traversed. Claims 16 and 30 have been amended to address the issues raised by the Examiner at paragraph 7 of the Office Action. For the reasons set forth above, Applicants respectfully request that the Section 112 rejections of Claims 16, 19-22, 24 and 30 be withdrawn.

The rejection of Claims 16-18, 24-26, and 30 under 35 U.S.C. § 112, second paragraph, is respectfully traversed. Claims 16, 25 and 30 have been amended to address the issues raised by the Examiner at paragraph 8 of the Office Action. For the reasons set forth above, Applicants respectfully request that the Section 112 rejections of Claims 16-18, 24-26 and 30 be withdrawn.

The rejection of Claims 16-19, 24, 28, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,061,668 to Sharrow (hereinafter referred to as "Sharrow") in view of U.S. Patent No. 5,825,890 to Elgamal et al. (hereinafter referred to as "Elgamal") and U.S. Patent No. 6,366,682 to Hoffman et al. (hereinafter referred to as "Hoffman") is respectfully traversed.

Applicants' respectfully traverse the Examiner's assertion on page 3 of the Office Action that "Elgamal further discloses changing the session key by storing a master key at both transmitting and receiving devices and using the master key to generate new session keys." Rather, Elgamal describes that "[t]he client delivers a master key to the server" (Col. 7, line 41), and "[t]he master key is used by the client and the server to produce session keys". (Col. 7, lines 43-44) As such, Elgamal does not describe or suggest changing a session key by storing a master key at both transmitting and receiving devices. *Delivering* a master key from a client to a server does not describe or suggest *storing* a master key at both a transmitting and receiving device. Further, *producing* a session key does not describe or suggest *changing* a pre-existing keying variable.

Sharrow describes a central management computer (10) that uses a data format to transmit instructions, acknowledgments, and messages to appliances and machines on a network (Col. 3, lines 12-16). The central management computer checks for an acknowledgment for each transmission sent, and sends an acknowledgment for every data transmission correctly received (Col. 3, lines 23-26). The data format used by the central management computer to transmit data includes a data field, a message, and a checksum to protect data integrity (Col. 3, lines 12-16, 20-22).

Hoffman describes a method to thwart resubmission attacks completely that uses only one sequence number module (SNM) validate packets (Col. 30, lines 31-32). Under this scheme, there is no update transmission delay window to exploit with a resubmission attack (Col. 30, lines 32-34). Alternately, multiple SNMs can be actived at the same time provided none of them handle sequence number validation for the same biometric input apparatus (BIA)-equipped device (Col. 30, lines 34-37).

Claim 16 recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication center and the first appliance; maintaining at the appliance communication center a second shared message counter that counts messages communicated

between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter; generating a first authentication word by applying an appliance message, a shared authentication keying variable, and the first shared message counter, as stored in the communication center, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and changing, within the first appliance, the shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word to authenticate the appliance message, the second authentication word is different from the appliance message."

None of Sharrow, Elgamal, and Hoffman, considered alone or in combination, describes or suggests a method for authenticating appliance messages as recited in Claim 16. Specifically, none of Sharrow, Elgamal, and Hoffman, considered alone or in combination, describes or suggests changing, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word to authenticate an appliance message, where the second authentication word is different from the appliance message, as required by Applicants' claimed invention. Rather, Sharrow describes transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal describes delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman describes activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Accordingly, none of Sharrow, Elgamal, and Hoffman, considered alone or in combination, describes or suggests changing, within the

first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word to authenticate an appliance message, where the second authentication word is different from the appliance message, as required by Applicants' claimed invention. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Elgamal and Hoffman.

Claims 17-19 and 24 depend, directly or indirectly, from independent Claim 16. When the recitations of Claims 17-19 and 24 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claims 17-19 and 24 likewise are patentable over Sharrow in view of Elgamal and Hoffman.

Claim 28 recites a system comprising "a first appliance including: a first shared message counter; a processor; and a memory coupled to the processor, the memory storing instructions for execution by the processor for: receiving an authenticated message, including a first authentication word and an appliance message, at the first appliance; generating a second authentication word by applying the first shared message counter, as stored in the first appliance, a shared authentication keying variable, and the appliance message to an authentication algorithm; and comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message; a second appliance separate from the first appliance; and an appliance communication center including a second shared message counter and a third shared message counter, the second shared message counter shared between the appliance communication center and the first appliance, the third shared message counter shared between the communication center and the second appliance, and the third shared message counter configured to provide a count separate from a count provided by the second shared message counter, wherein the memory configured to store instructions to change, within the first appliance, the shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the shared authentication keying variable is used to generate the second authentication word."

None of Sharrow, Elgamal, and Hoffman, considered alone or in combination, describes or suggests a system as recited in Claim 28. Specifically, none of Sharrow, Elgamal, and Hoffman, considered alone or in combination, describes or suggests the memory configured to store instructions to change, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate the second authentication word, as required by Applicants' claimed invention. Rather, Sharrow describes transmitting data by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal describes delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman describes activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Accordingly, none of Sharrow, Elgamal, and Hoffman, considered alone or in combination, describes or suggests the memory configured to store instructions to change, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate the second authentication word, as required by Applicants' claimed invention. For the reasons set forth above, Claim 28 is submitted to be patentable over Sharrow in view of Elgamal and Hoffman.

Claim 29 depends from independent Claim 28. When the recitations of Claim 29 are considered in combination with the recitations of Claim 28, Applicants submit that dependent Claim 29 likewise is patentable over Sharrow in view of Elgamal and Hoffman.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claims 16-19, 24, 28, and 29 under 35 U.S.C. §103(a) be withdrawn.

The rejection of Claims 25, 27, 30, and 31 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow in view of Elgamal, Hoffman, and "Commercial Laundry Services", available at http://www.cinetworks.com/~jetz/comrcl.html (hereinafter referred to as "Commercial Laundry Services"), is respectfully traversed.

Sharrow, Elgamal, Hoffman are described above.

Commercial Laundry Services describes a JETZ equipment that includes a temper-resistant vault. The JETZ equipment also includes a non-resettable counter which insures accountability.

Claim 25 recites a system comprising "a plurality of appliances including a first appliance and a second appliance; and an appliance communication center including: network connections terminating at the appliances; a processing circuit; a memory storing a plurality of shared counters including a first shared message counter and a second shared message counter, the first shared message counter shared between the appliance communication center and the first appliance, the second shared message counter shared between the communication center and the second appliance, the first shared message counter configured to provide a count separate from a count provided by the second shared message counter, the first and second shared message counters configured to be non-resettable, the memory further storing instructions for: maintaining at the appliance communication center the first shared message counter; generating a first authentication word by applying an appliance message, a shared authentication keying variable, and the first shared message counter, as stored in the appliance communication center, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and transmitting a command to change, within the first appliance, the shared authentication keying variable, wherein the shared authentication keying variable is changed by installing a master keying variable within the first appliance and the appliance communication center, and the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word."

None of Sharrow, Elgamal, Hoffman, and Commercial Laundry Services, considered alone or in combination, describes or suggests a system as recited in Claim 25. Specifically, none of Sharrow, Elgamal, Hoffman, and Commercial Laundry Services, considered alone or in combination, describes or suggests the memory further storing instructions for transmitting a command to change, within the first appliance, a shared authentication keying variable, where the shared authentications keying variable is changed by installing a master keying variable within the first appliance and the appliance communication center, and the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word, as required by Applicants' claimed invention. Rather, Sharrow describes transmitting data by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal describes delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman describes activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Commercial Laundry Services describes insuring accountability by using a non-resettable counter. Accordingly, none of Sharrow, Elgamal, Hoffman, and Commercial Laundry Services, considered alone or in combination, describes or suggests the memory further storing instructions for transmitting a command to change, within the first appliance, a shared authentication keying variable, where the shared authentication keying variable is changed by installing a master keying variable within the first appliance and the appliance communication center, and the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word, as required by Applicants' claimed invention. For the reasons set forth above, Claim 25 is submitted to be patentable over Sharrow in view of Elgamal, Hoffman, and Commercial Laundry Services.

Claim 27 depends from independent Claim 25. When the recitations of Claim 27 are considered in combination with the recitations of Claim 25, Applicants submit that dependent

Claim 27 likewise is patentable over Sharrow in view of Elgamal, Hoffman, and Commercial Laundry Services.

Claim 30 recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at a first appliance a first non-resettable shared message counter, the first non-resettable shared message counter shared between the first appliance and a remotely located appliance communication center; maintaining at the appliance communication center a second non-resettable shared message counter that counts messages communicated between the appliance communication center and the first appliance; maintaining at the appliance communication center a third non-resettable shared message counter that counts messages communicated between the appliance communication center and a second appliance, the third non-resettable shared message counter provides a count separate from a count provided by the second non-resettable shared message counter; generating a first authentication word by applying an appliance message, a shared authentication keying variable, and the first non-resettable shared message counter, as stored in the first appliance, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center; and changing, within the first appliance, the shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the shared authentication keying variable is used to generate the first authentication word to authenticate the appliance message."

None of Sharrow, Elgamal, Hoffman, and Commercial Laundry Services, considered alone or in combination, describes or suggests a method for authenticating appliance messages as recited in Claim 30. Specifically, none of Sharrow, Elgamal, Hoffman, and Commercial Laundry Services, considered alone or in combination, describes or suggests changing, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate the first authentication word to authenticate the appliance message, as required by Applicants' claimed invention. Rather, Sharrow describes transmitting data by using a data format including a data field, a

message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal describes delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman describes activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Commercial Laundry Services describes insuring accountability by using a non-resettable counter. Accordingly, none of Sharrow, Elgamal, Hoffman, and Commercial Laundry Services, considered alone or in combination, describe or suggest changing, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate the first authentication word to authenticate the appliance message, as required by Applicants' claimed invention. For the reasons set forth above, Claim 30 is submitted to be patentable over Sharrow in view of Elgamal, Hoffman, and Commercial Laundry Services.

Claim 31 depends from independent Claim 30. When the recitations of Claim 31 are considered in combination with the recitations of Claim 30, Applicants submit that dependent Claim 31 likewise is patentable over Sharrow in view of Elgamal, Hoffman, and Commercial Laundry Services.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claims 25, 27, and 30-31 under 35 U.S.C. 103(a) be withdrawn.

The rejection of Claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow in view of Elgamal, Hoffman, and further in view of Kaufman (*Network Security: Private Communication in a Public World*) (hereinafter referred to as "Kaufman"), is respectfully traversed.

Sharrow, Elgamal, and Hoffman are described above.

Kaufman describes a system that avoids an implausible attack (page 242, third paragraph). The system avoids the attack by using sequence numbers in different ranges for two directions, by having a DIRECTION BIT somewhere in a message, or by having an integrity code computed by some subtly different algorithm in the two directions (page 242, third paragraph).

Claim 20 depends indirectly from Claim 16, which recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication center and the first appliance; maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter; generating a first authentication word by applying an appliance message, a shared authentication keying variable, and the first shared message counter, as stored in the communication center, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and changing, within the first appliance, the shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word to authenticate the appliance message, the second authentication word is different from the appliance message."

None of Sharrow, Elgamal, Hoffman, and Kaufman, considered alone or in combination, describes or suggests a method for authenticating appliance messages as recited in Claim 16. Specifically, none of Sharrow, Elgamal, Hoffman, and Kaufman, considered alone or in combination, describes or suggests changing, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is

used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message, as required by Applicants' claimed invention. Rather, Sharrow describes transmitting data by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal describes delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman describes activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Kaufman describes using a plurality of sequence numbers in different ranges for two directions, having a DIRECTION BIT somewhere in a message, or having an integrity code computed by some subtly different algorithm in the two directions. Accordingly, none of Sharrow, Elgamal, Hoffman, and Kaufman, considered alone or in combination, describes or suggests changing, within the first appliance, a shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the shared authentication keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message, as required by Applicants' claimed invention. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Elgamal, Hoffman, and further in view of Kaufman.

When the recitations of Claim 20 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claim 20 likewise is patentable over Sharrow in view of Elgamal, Hoffman, and further in view of Kaufman.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claim 20 under 35 U.S.C. §103(a) be withdrawn.

Moreover, Applicants respectfully submit that the 35 U.S.C. § 103 rejections of Claims 16-20, 24, 25, and 27-31 are not proper rejections. As is well established, obviousness cannot be established by combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. None of Sharrow, Elgamal, Hoffman, Commercial Laundry Services, or Kaufman, considered alone or in combination, describes or suggests the claimed combination. Further, in contrast to the Examiner's assertions within the Office Action, Applicants respectfully submit that it would not be obvious to one skilled in the art to combine Sharrow with Elgamal, Hoffman, Commercial Laundry Services, or Kaufman because there is no motivation to combine the references suggested in the art.

As the Federal Circuit has recognized, obviousness is not established merely by combining references having different individual elements of pending claims. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP §2143.01. Rather, there must be some suggestion, outside of Applicants' disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicants' disclosure. In re Vaeck, 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case, neither a suggestion or motivation to combine the prior art disclosures, nor any reasonable expectation of success has been shown.

Further, it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the cited art so that the claimed invention is rendered obvious. Specifically, one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the art to deprecate the claimed invention. Further, it is impermissible to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. The present 35 U.S.C. § 103 rejections are based on a combination of teachings selected from multiple patents in an attempt to arrive at the claimed invention. Specifically, Sharrow describes transmitting data by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data

transmission correctly received. Elgamal describes delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman describes activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Commercial Laundry Services describes insuring accountability by using a non-resettable counter. Kaufman describes using a plurality of sequence numbers in different ranges for two directions, having a DIRECTION BIT somewhere in a message, or having an integrity code computed by some subtly different algorithm in the two directions. Otherwise, there is a possibility of running out of the sequence numbers during the conversation. Because there is no teaching nor suggestion in the cited art for the combination, the 35 U.S.C. § 103 rejections appear to be based on a hindsight reconstruction in which isolated disclosures have been picked and chosen in an attempt to reject the claims of the present application. Of course, such a combination is impermissible, and for this reason Applicants request that the 35 U.S.C. § 103 rejections of Claims 16-20, 24, 25, and 27-31 be withdrawn.

The objection to Claims 21 and 22 is respectfully traversed. Claims 21 and 22 depend from Claim 16, which Applicants submit is patentable for at least the reasons presented above. When the recitations of Claims 21 and 22 are considered in combination with the recitations of Claim 16, Applicants submit that Claims 21 and 22 are likewise patentable over the cited art. For the reasons set forth above, Applicants request that the objection to Claims 21 and 22 be withdrawn.

Newly added Claim 32 depends from independent Claim 16, which Applicants submit is patentable for at least the reasons presented above. When the recitations of Claim 32 are considered in combination with the recitations of Claim 16, Applicants submit that Claim 32 likewise is patentable over the cited art.

In view of the foregoing amendments and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,

Eric T. Krischke
Registration No. 42,769
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070